How to Set Up a Burner Phone
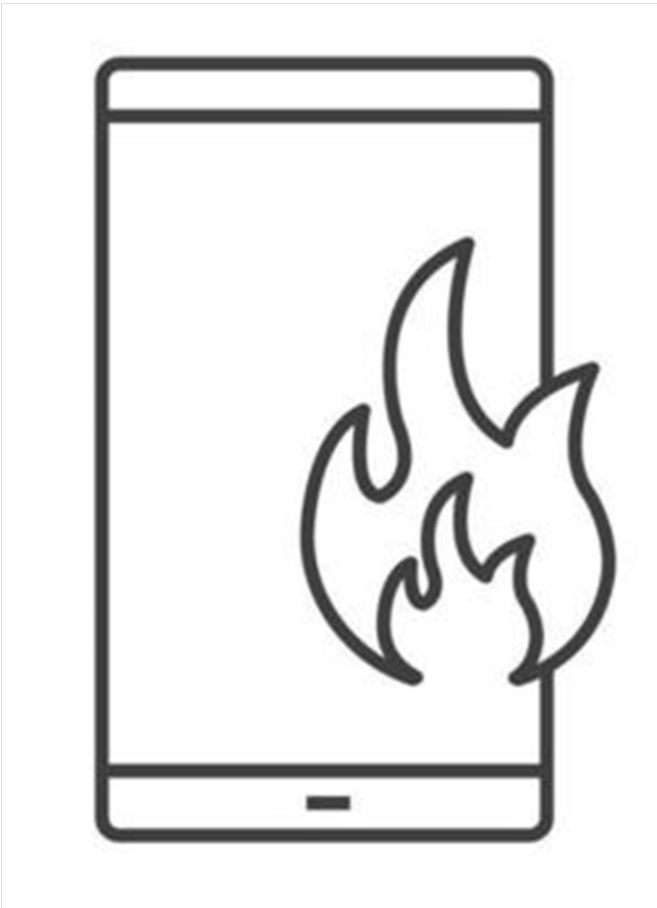
March 2023

Table of Contents

Introduction

A burner phone is a temporary phone typically used for a specific purpose or time period. If you are traveling to a frontline/eco-defense space, getting involved in anarchist or other organizing projects, and/or planning actions that may require anonymous communications, you may want a burner phone.

Maybe you've heard people talk about burner phones before and know a little bit about them, but don't know how to get one and set it up. That's what this zine is about. Step by step, start to finish, how to acquire a phone and dispose of it when it's time for it to be "burned." This guide was developed for anarchists engaged in organizing or action spaces, in light of their need to evade state surveillance and repression. However, the information may be useful to others outside that context as well.

This is not a general introduction to smartphones. If you are new to phones or have not used an Android device before, it might be worthwhile to look up basic tutorials or ask a friend for help. Every phone is slightly different, so some menu options or settings may be in different places than what is written in this guide.

Of course, only you know your specific security needs. Depending on your technology use, threat model(s), types of communication, people with whom you communicate, and other factors, some of the information and recommendations here may be more

or less suited to your needs. That being said, if you do not know enough about technology or security to understand what different choices could mean, I suggest choosing the more secure options until you are able to fully weigh the pros and cons of those choices.

Also remember that your actions affect more than just you: poor security affects everyone in your network and could compromise the safety or security of others. Security culture is only as strong as its weakest links. Consider having conversations about security needs and norms with comrades and affinity groups so you are all on the same page.

**General phone security tips that also apply to a burner phone:**

- Choose a strong password: alphanumeric (mix of letters and numbers), not a common phrase, different from your password on any other accounts or devices. Not a PIN. Not Face ID. Not fingerprint unlock. PASSWORD.
- If participating in activities for which it is imperative that you are not monitored in any way (GPS, audio, video), leave the phone elsewhere.

- The only way to ensure the phone is not transmitting location data is to turn it off and remove the battery. Just airplane mode is NOT sufficient. Turning it off is NOT sufficient.
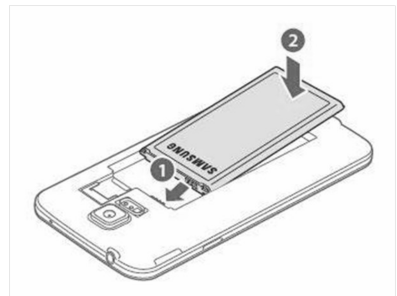
Seriously. Take out the battery or leave it somewhere else if you do not want your location tracked. Faraday bags are also an option: they block signals from being sent to or from the phone.

- If something is extremely sensitive, consider not writing it down or sending it in any way. While risk of monitoring content and/or connecting it to a specific individual can be minimized, the risk is never zero. Communicating in person, without phones, in a location that is extremely unlikely to be monitored is the most secure way to transmit information. (Though, of course, that is not always possible; that's why this guide exists.)
- Use the burner phone minimally. This includes real-world tasks where a phone is not really necessary and reducing use of the phone to minimize compilation of data that could be traced back to you, the user. Don't log in to personal accounts and avoid making accounts for anything, as much as possible. If you must make an account, use a throwaway email or fake information.
- Photos and videos contain metadata including location and information about your device. Sending photos through Signal removes metadata, but emailing or uploading to a website might not. Use an exif or metadata remover like verexif.com to remove metadata from photos.
- If you think your phone may be seized, turn it off! If you have time, consider deleting signal or doing a factory reset as well. But, at minimum, turn it OFF.

Some attention to security is better than none. Even if you don't feel prepared to do all of these steps, making information about yourself harder to find (if not impossible) and reducing inc riminating evidence (if not eliminating it completely) are still useful. It can be overwhelming to try to do everything all at once; don't let that persuade you into giving up completely.
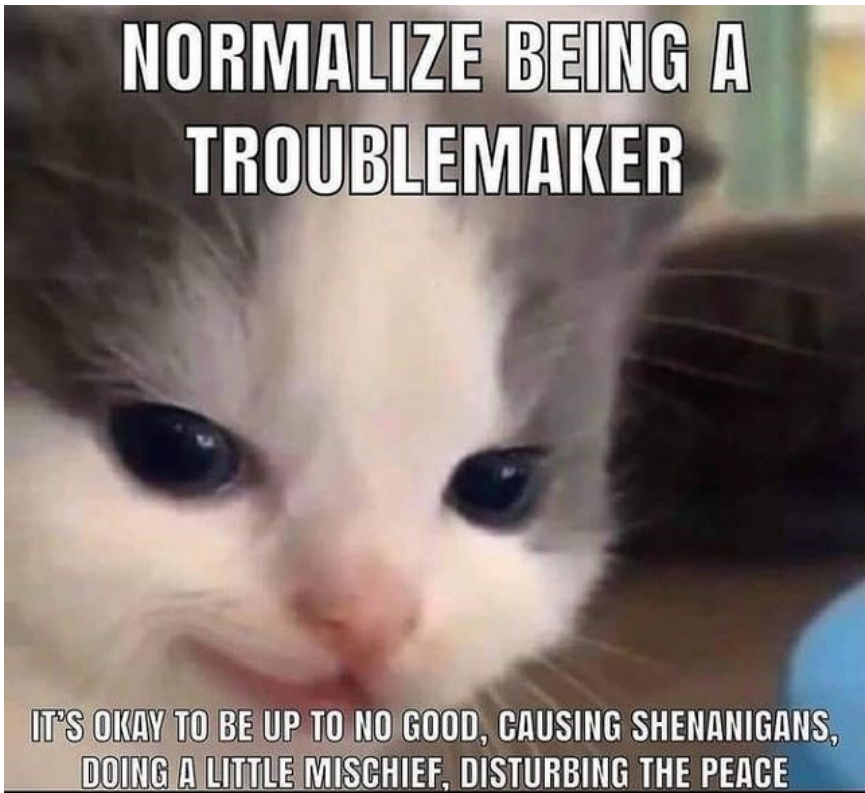
Acquire the Phone

Consider the purpose of your new burner phone: do you need it for standard (unencrypted) calls or texts and nothing else? A flip phone might be what you want. Are you trying to use signal or other encrypted messaging, apps, the internet, GPS navigation, and everything else that comes with a smartphone? That may be what you need. Prices for the cheapest flip phone or smartphone are comparable; in my experience the smartphone is usually around $10-15 more. The price of service plan depends on how much data and how many minutes you want; the type of phone is irrelevant.

No-Contract phones available at Walmart and many other big box retailers. Pay in cash, cover up as much as you feel comfortable with special attention to identifying marks (eg tattoos). Leave your personal phone elsewhere!

Select the phone you want and a compatible plan. Plans come on prepaid cards which are displayed above the corresponding phones. Make sure the phone and card are from the same company.

Activate the Phone

You will need to be in a place with wifi to set up your new burner phone. Some common places include fast food restaurants, cafés, or even the Walmart parking lot. If you want the phone to remain unconnected to your identity and other devices, do not activate it in your home or any other place you frequent. Also make sure you do not have your personal phone in the same place as the burner when you activate it.

If you are traveling to the location where you intend to use your new burner phone, consider activating it in that local area. For example, if I live in Colorado but want a burner to use mostly in California, activating it in Colorado and traveling with it activated could give away the information that I started in Colorado and went to California. However, if I activate it when I arrive in California (or somewhere else along the way), my starting/home location remains unknown.

Your new phone should come with activation instructions. Typically you have to go to a website to enter the phone information and plan information. Sometimes you can also activate your plan by calling a company number from the new phone.

If you must make an account or provide an email address, do not use any information connected to your real world identity! Guerrillamail.com and Tempr.email provide temporary, anonymous, disposable email addresses. If you don't want to keysmash or if you need to create a memorable username and password, consider using a random word generator and write the information down somewhere secure (if you want to save it).

Phone Setup

If setting up a flip phone, you've done it! There are fewer steps because there are fewer features. For more information on using a burner flip phone securely (since you can't use encrypted messaging apps or secure websites), check out Burner Phone Best Practices : A User's Guide from CrimethInc (https:// crimethinc.com/2017/03/27/ burner-phone-best-practices).

If you are setting up a smartphone:

1. Charge your new phone and turn it on.

2. Press "Start" on the homescreen to begin.

3. When asked to create a Google account, don't! You can select "Skip" in the bottom left of the screen and avoid this completely.

4. Deny all permissions or optional data reporting. You must accept the terms of service to use the device, but everything else can be declined.

5. The default screen lock is a PIN, which is likely NOT sufficient for your security needs. If you set a PIN, change it immediately once you get through the setup menu. Face ID is even worse; decline this option.

6. Once setup is complete and you reach the phone homescreen, delete all apps you do not need. These probably include many Google products (Drive, Video, Gmail), pre-installed social media (Facebook, TikTok), and mobile games (Candy Crush, Ball Sort).

7. Swipe up on the screen to view all apps. Press and hold an app icon then select "App Info". Then, on the settings screen that appears, select "Uninstall" or "Disable" (some apps cannot be uninstalled based on manufacturer settings).

Apps to Get

After you have removed all of the apps you do not need or want, it is time to install the apps you actually will use. In general, it is best to install the absolute minimum of what you might need.

The following pages have a table summarizing my recommendations. Following the table are detailed instructions to download each of these apps without creating a Google account or using the Google Play Store.

App to Install	Purpose	Instead of
F-Droid	Find and download apps	Google Play Store, APK Pure
Signal	Encrypted messaging	SMS, TextNow, TextFree, WhatsApp, Messenger...
Orbot	Proxy that routes all your phone's internet traffic through Tor	n/a
VPN (Riseup, Mulvad, etc.)	Makes your phone's internet traffic appear to come from a different geographic location	Orbot, if desired

DuckDuckGo Browser	Standard everyday browser with minimal tracking	Chrome Browser, Firefox, Opera
Tor Browser	Access the internet more securely and anonymously	Chrome Browser, Firefox, Opera
Simple Keyboard	Replacement keyboard so your words and keystrokes are not monitored	Gboard, standard pre-installed keyboard
Organic Maps	Maps & navigation	Google Maps, Waze, Open Street Maps
NewPipe	Watch YouTube videos without an account or tracking	YouTube
ViMusic	Listen to music without an account or tracking	Spotify, Pandora, free radio apps

In order to avoid creating a Google account on your new phone, here is the series of steps to install and begin using all of these apps securely:

F-Droid

1. Open your browser and go to https://f-droid.org/.

2. Press the button that reads "Download F-Droid"

3. After the apk file has been downloaded, install the app. Depending on your specific phone, it could be easiest to swipe down from the top of the screen, tap the download notification, and select "install." Or navigate to Files > Downloads > F-Droid.apk and tap to install.

4. Your phone may give you a notification saying its security permissions are blocking app installations from "this source" (Chrome, or your default browser). If this happens, select "install anyway" and allow permissions in the popup settings menu that appears.

That's it! You should now have F-Droid running on your phone. If the app begins having issues (for example, all downloads being cancelled or getting error notifications), uninstall and reinstall using these same steps.

F-Droid

APPS   FORUM   DOCS   NEWS   ISSUES

CONTRIBUTE   ABOUT

What is F-Droid?

F-Droid is an installable catalogue of FOSS (Free and Open Source Software) applications for the Android platform. The client makes it easy to browse, install, and keep track of updates on your device.
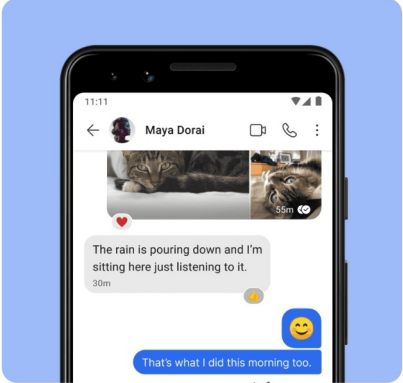
DOWNLOAD F-DROID

PGP Signature

Signal

1. In your browser, go to https://signal.org/android/ apk

2. Scroll down to the button that says "Download" and press it.

3. Install the app by swiping down from the top of the screen, tapping the download notification, and selecting "install." Or, if you prefer, navigate to Files > Downloads > Signal-Android-website-prod-universal-release-6.13.7.apk (file name may vary slightly as new versions are released) and tap to install.

4. When you open Signal, you will have the option to transfer your account or make a new one—make a new one!

It is easiest to use the phone number associated with the SIM of your new phone, but if you have a VoIP number or

Signal Android APK

Website distribution build

Danger zone

Advanced users with special needs can download the Signal APK directly. Most users should not do this under normal circumstances.

Signal 6.13.8

Download

You can verify the signing certificate on the APK matches this SHA256 fingerprint:

```
29:F3:4E:5F:27:F2:11:B4:24
EA:FB:A2:DA:35:AF:35:C1:64
```

*additional phones you could consider using one of
those numbers instead.*

5. Signal will give you the option to set a recovery
   pin. Do not do this! Press "Skip" in the bottom
   left corner of the screen.

*A recovery pin could allow the content of your signal
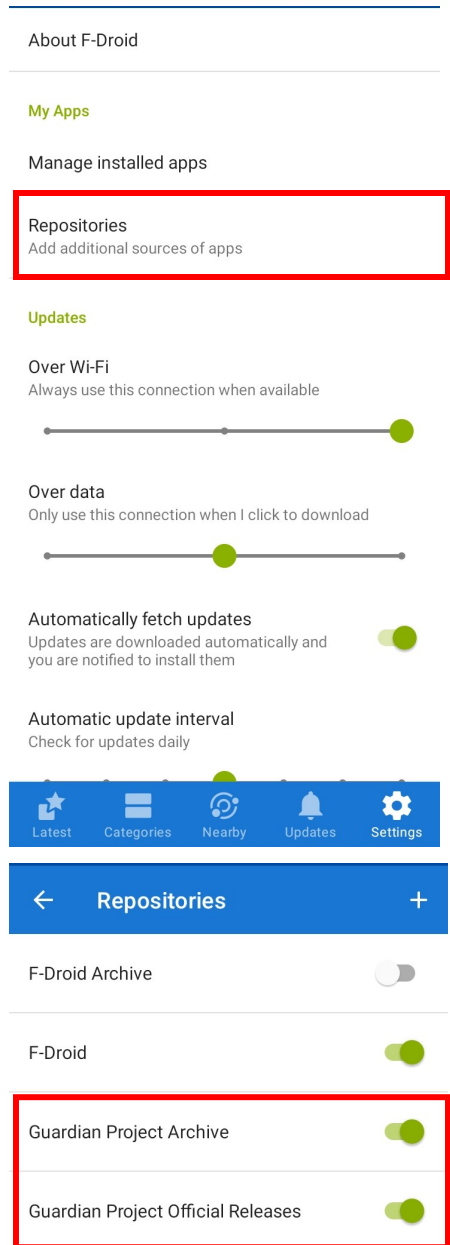messages to be transferred to another device.
Assuming you are using this phone to remain
anonymous and keep your communications more
secure, it is best to keep your signal account tied
to only your burner device. This does mean that if
the app is deleted or the phone is lost then all the
messages are gone as well. However, this may
actually be a benefit if your phone falls into the
wrong hands.*

6. When setting your name and profile picture, do
   not use real-world or social media info.

*I have seen people in large public chats (which are
likely to include police or other law enforcement/
surveillance agencies) use all of the following in
their signal profile: profile picture of their actual
unedited face, legal name or everyday chosen name
(sometimes called "civ name": the name you are
known by in most places) and social media handle
in name or bio. Sometimes people also use their
signal name, profile picture, and/or bio to make
spicy jokes about c rimes. I would recommend
against all of these. Your friends will know who you
are when you give them your number; a burner
signal account should not be treated as social media.*

Orbot & Tor Browser

1. Open F-Droid and go to "Settings" (gear icon in bottom right).

2. Tap "Repositories"

3. Tap the sliders next to "Guardian Project Archive" and "Guardian Project Official Releases" to activate those options. The slides should change from gray to green when activated.

4. Return to the F-Droid homepage ("Latest" tab) by pressing the back button or closing and re-opening the app.

5. Swipe down on the screen to refresh. A gray bar that says "Updating Repositories" may appear at the top of the screen; wait for the app to finish loading.

About F-Droid

My Apps

Manage installed apps

Repositories
Add additional sources of apps

Updates

Over Wi-Fi
Always use this connection when available

Over data
Only use this connection when I click to download

Automatically fetch updates
Updates are downloaded automatically and you are notified to install them

Automatic update interval
Check for updates daily

| Latest | Categories | Nearby | Updates | Settings |

← **Repositories** +

F-Droid Archive

F-Droid

Guardian Project Archive

Guardian Project Official Releases

6. Press the green magnifying glass icon (bottom right) to search for Tor Browser for Android (or Orbot, whichever you want to install first). You may need to scroll to find the app you are looking for. (The "Alpha" version is also fine.)

Tor Browser icon

7. Tap the app you want to open its page. Make sure the byline on the app page says "by The Tor Project" or "by Guardian Project" and has been updated within the past couple months.

Orbot app icon

8. Press the blue button that says "Install" to download the app. When a popup appears that asks if you want to install the app, select "Install".

9. If a popup appears saying security permissions are blocking app installations from "this source" (F-Droid), select "install anyway" and allow permissions in the popup settings menu that appears.

10. The first time you open Orbot, you may get a popup asking to allow Orbot to set up a VPN connection. Select "OK".

11. To use Orbot, open the app and tap the onion icon. When activated, the icon will turn green and the word "Stop" will appear. You should also see a small key icon appear in the top right of your phone screen near the wifi and cell service signals. Tap the onion again to deactivate Orbot.

12. If you want to ensure your internet traffic is always routed through Tor (via Orbot), you can adjust your phone settings. Go to Settings > Connections > VPN > Orbot (gear icon) and tap the slider next to "Always-on VPN". You can also double check the VPN is on by looking for the key icon mentioned in Step 11.

Connection request

Orbot wants to set up a VPN connection that allows it to monitor network traffic. Only accept if you trust the source.

⚷ appears at the top of your screen when VPN is active.

CANCEL   OK

Note that if you activate always-on VPN , your phone will not connect to internet without protection. You must have Orbot (or another VPN) running if you wish to connect to the internet.

DuckDuckGo Browser

1. Open F-Droid and tap the green magnifying glass icon to search for "DuckDuckGo Browser".

2. Tap the app icon and press the blue button that says "Install".

3. When you first open the app, your phone may ask if you want to change your default browser to DuckDuckGo. I recommend changing your default browser then deactivating Google Chrome.
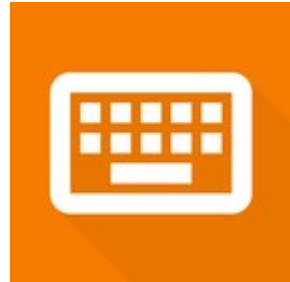
No additional setup or setting adjustments are needed to use this app.

Simple Keyboard

1. Open F-Droid and tap the green magnifying glass icon to search for "Simple Keyboard".

You are looking for the app with an orange keyboard icon made by Tibor Kaputa. They have a whole suite of "Simple Mobile Tools" apps including calendar, voice recorder, notes, calculator and more.
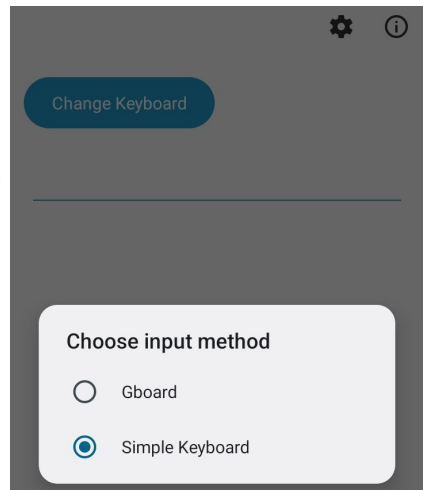
2. Tap the app icon and press the blue button that says "Install".

3. When you first open the app, you will see a blue button that says "Change Keyboard". Press it.

4. In the menu that comes up, there will be the option to "Choose input method". Select "Simple Keyboard".

5. You may need to restart your phone for this change to take effect.

Organic Maps

1. Open F-Droid and tap the green magnifying glass icon to search for "Organic Maps".

2. Tap the app icon and press the blue button that says "Install".

3. When you first open the app, it will ask you to download World Map. Do this, as it is required for setup.

After installing World Map, you will have a general outline of all continents. Assuming you want to use this app for its offline maps, you will need to download more maps in specific areas.

5. You may also be asked for location permissions. The most secure option is to deny location permissions, but any option here is likely fine. If you intend to use GPS navigation on your phone, precise location will be required.

6. Tap the gray icon with three parallel horizontal lines in the bottom right, then select "Download Maps."

From this menu, you can select offline maps of many regions in most countries. I suggest downloading only the maps you think you are likely to use.

7. Maps are organized by country then region. To download additional maps, press the blue circle

with a "+" icon in the bottom right of the screen. From there, you can search for the regions you want to download.

For example, if I wanted to navigate offline in the state of Montana, I could search "Montana" or search "United States" then "Montana" within that folder. Then I could select any or both of the regional maps available for Montana (in this case, the state is split into East and West). If you plan to travel many places with this phone or are unsure which locations you need, consider downloading additional maps.

Note that Organic Maps does not have as much detailed information as other apps or websites you may be used to, like Google Maps. Searching for locations in the app may or may not work. Sometimes it will find the street, but not a specific address. If you search for a store by name (like "Home Depot"), it may not bring up the nearest one. Some regions have better data than others.

If you need to search for locations, consider using Google Maps through your browser (maps.google.com) or another online option to find the exact address of the place you want to go. If Organic Maps is unable to find the place by street name and number, use an address to GPS converter like gps-coordinates.org or addresstogps.com. Some aspects of security include sac rificing convenience; consider your specific needs and whether these tradeoffs make sense for you.

Additional Apps (from F-Droid)

Installing additional apps from F-Droid is similar to how you would use any other app store. If you don't like Orbot or sometimes want to sacrifice some security for loading additional website features, I suggest installing a VPN like RiseUp or Mulvad. There are many other VPN options as well; this guide is not an in-depth analysis of their features and drawbacks.

If you expect to want to use YouTube and/or listen to music, I also suggest NewPipe and ViMusic.

You can also look through the apps available on F-Droid and download whatever you think seems interesting and useful. In general, having fewer apps keeps your device more secure: there are fewer opportunities for attack or infiltration and less data available about you, the user.
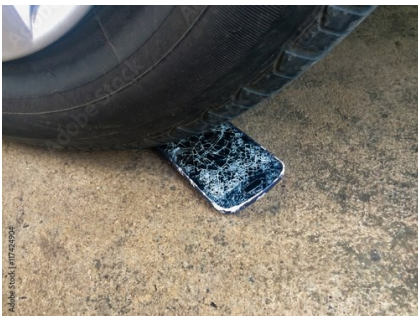
Dispose of the Phone

The point of a burner is that you get rid of it when you are done (it becomes "burned"). This does not have to literally involve fire (and maybe shouldn't... some of the chemicals may be toxic if burned), but just means you stop using the phone and destroy it.

1. Delete everything from the phone. Navigate to Settings > System > Reset > Erase all data (factory reset)

2. After ensuring the reset is complete, remove the battery and SIM card from the phone.

3. Destroy the actual phone: run it over with a car, hit it with a hammer, do whatever seems fun. SIM cards can be cut with strong scissors or wire cutters.

4. Dispose of the physical phone and SIM card in places they are unlikely to be found, and extremely unlikely to be connected to you. Think random city trash can, dumpster, buried in the woods somewhere far away from your usual location and wherever you used the phone. Dispose of the phone and SIM card in separate places.

5. The battery could be saved and re-used if you or someone you know has a compatible phone. Sometimes it's helpful to have a backup battery. However, if you don't have a use for it, I would recommend disposing of that as well. If found in your possession, it could narrow down a range of phone models you may have had.

Some of this may seem wasteful, and in some ways it is, but getting rid of items is the best way to ensure they are not connected to you. It is better to buy a new phone every once in a while and waste some plastic than to allow surveillance agencies or other bad actors to gather data on you or connect you to clandestine activities. Stay safe, be dangerous. <3

Additional Resources

Audio & Video:

Error451 from The Final Straw (22m)

- https://archive.org/details/tfsradio-Error451n02

How to be Anonymous in a Protest by The Hated One (YouTube—21m)

- https://www.youtube.com/watch?v=vMJH-UJyENs

Protestors, Here's How to Set Up a Cheap Burner Phone from The Intercept (21m)

- https://theintercept.com/2020/06/15/protest-tech-safety-burner-phone/

Articles & Zines (Short-form written media):

Burner Phone Best Practices from CrimethInc

- https://crimethinc.com/2017/03/27/burner-phone-best-practices

What Is a Burner Phone, and When Should You Use One? from How-To Geek

- https://www.howtogeek.com/712588/what-is-a-burner-phone-and-when-should-you-use-one/

Privacy Breakdown of Mobile Phones from Surveillance Self-Defense/Electronic Freedom Foundation

- https://ssd.eff.org/playlist/privacy-breakdown-mobile-phones

Mobile Phone Security for Activists and Agitators from Sprout Distro

- https://www.sproutdistro.com/catalog/zines/security/mobile-phone-activists/

Books/Long-form written media:

Rebel Alliance Tech Manual

- https://github.com/rebel-tech/Rebel-Alliance-Tech-Manual

Extreme Privacy: What It Takes to Disappear by Michael Bazzell

- (available wherever you regularly find free books online, or purchase)